

# Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 1b)

Vorlesung im Sommersemester 2016  
an der Universität Ulm  
von Bernhard C. Witt

# 1. Grundlagen des Datenschutzes

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes		Anforderungen zur IT-Sicherheit
→	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
	Technischer Datenschutz		Risiko-Management
	Kundendatenschutz		Konzeption von IT-Sicherheit

- Subsidiarität
- Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Transparenz
- Datenminimierung & begrenzte Speicherung
- Verhältnismäßigkeit
- Angemessene Sicherheit → Teil 1c
- Betroffenenrechte
- Abgrenzungen
- Datenschutzkontrolle

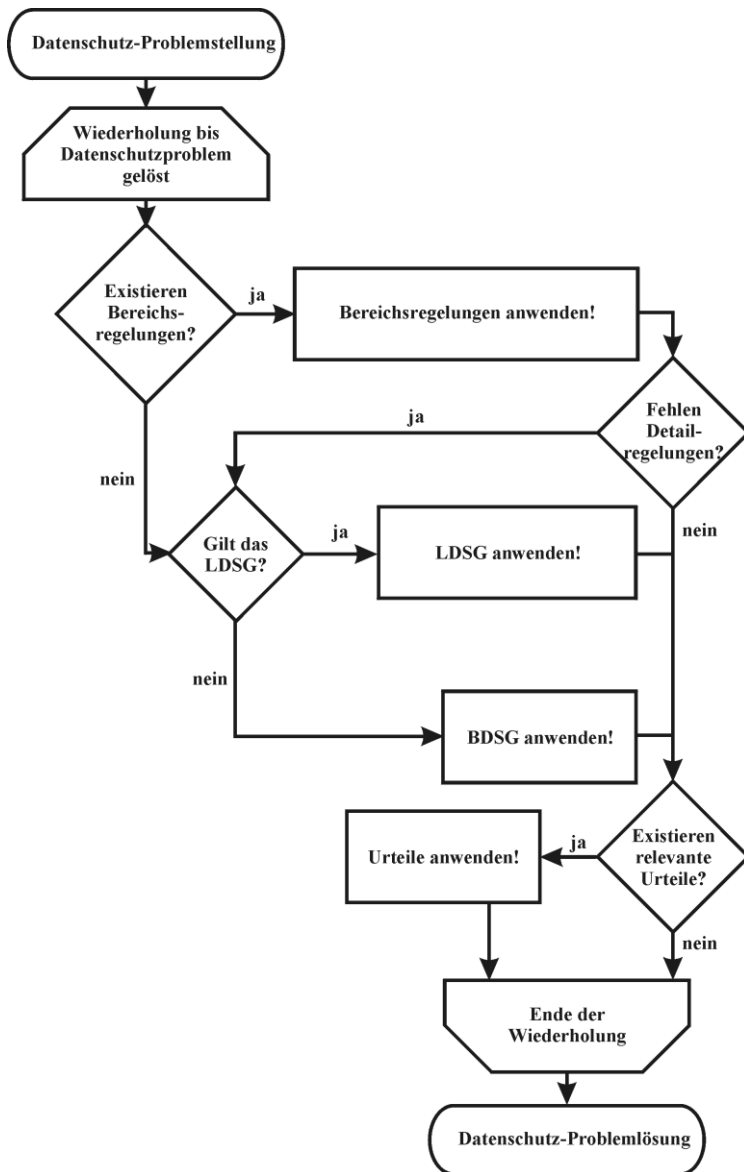
# Subsidiaritätsprinzip

resultierend aus der Normenklarheit:

- **bereichsspezifische** Regelungen haben immer **Vorrang** vor allgemeinen Regelungen
- fehlende Regelungen des Bereichsrechts werden durch entsprechende Regelungen des **Allgemeinrechts aufgefangen**
- gesetzliche Regelungen stehen in **Hierarchie** zueinander (u.U. aufgelöst durch Verbindung verschiedener Rechtsnormen oder gegenseitige Verdrängung), Lücken durch **Richterrecht** geschlossen

in der EU-DS-GVO dadurch umgesetzt, dass es nationalen Gesetzgebern gestattet ist, spezifischere Bestimmungen zu erlassen, die eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten (Art. 6 Abs. 2+3 der EU-DS-GVO)

# Subsidiarität: Anzuwendendes Recht in D (vor Wirksamkeit der EU-DS-GVO)



# Abgrenzung BDSG & LDSGGe

**BDSG:** Anwendung für

- Unternehmen
- Bundesbehörden
- Behörden im Wettbewerb

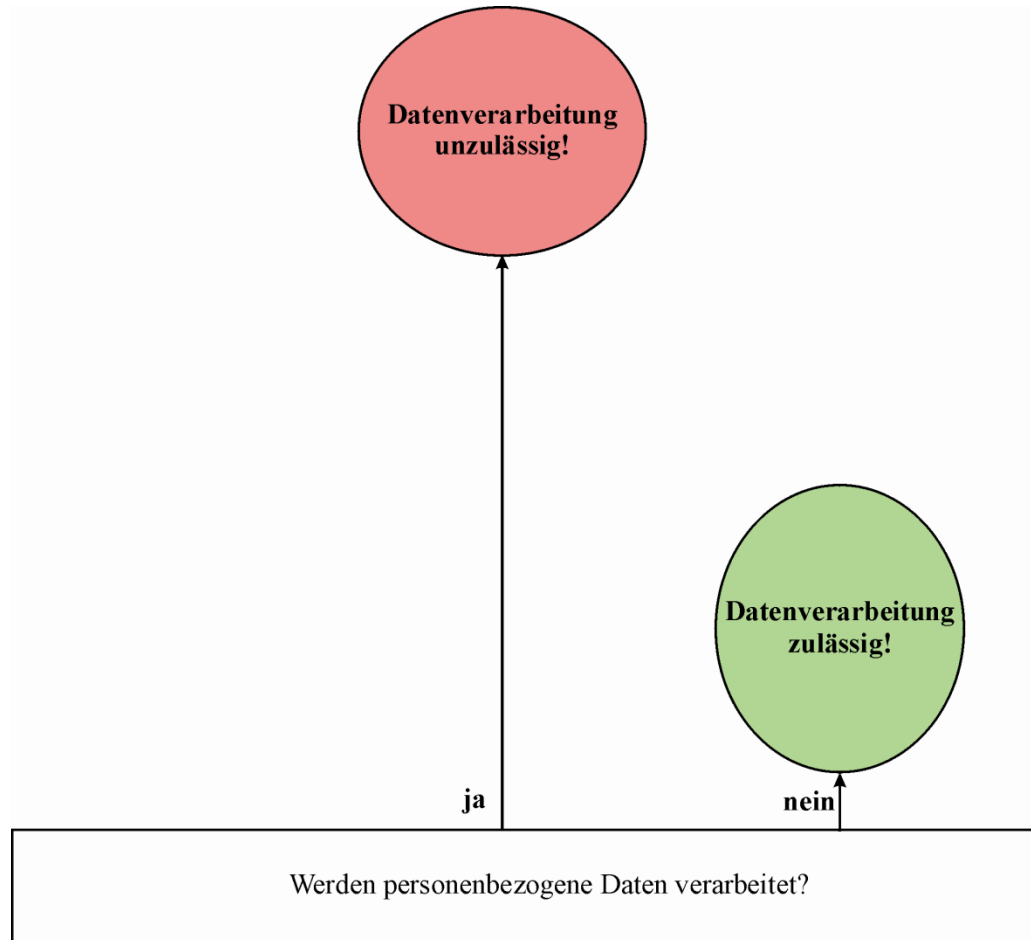
**LDSGGe:** Anwendung für

- Landesbehörden
- kommunale Behörden

**keine Anwendung (weder BDSG noch LDSG), wenn DV der ausschließlichen persönlichen bzw. familiären Tätigkeit dient!**

**Grundsatz: lex specialis hat Vorrang! [→ Subsidiarität!]**

# Verbot mit Erlaubnisvorbehalt (1)

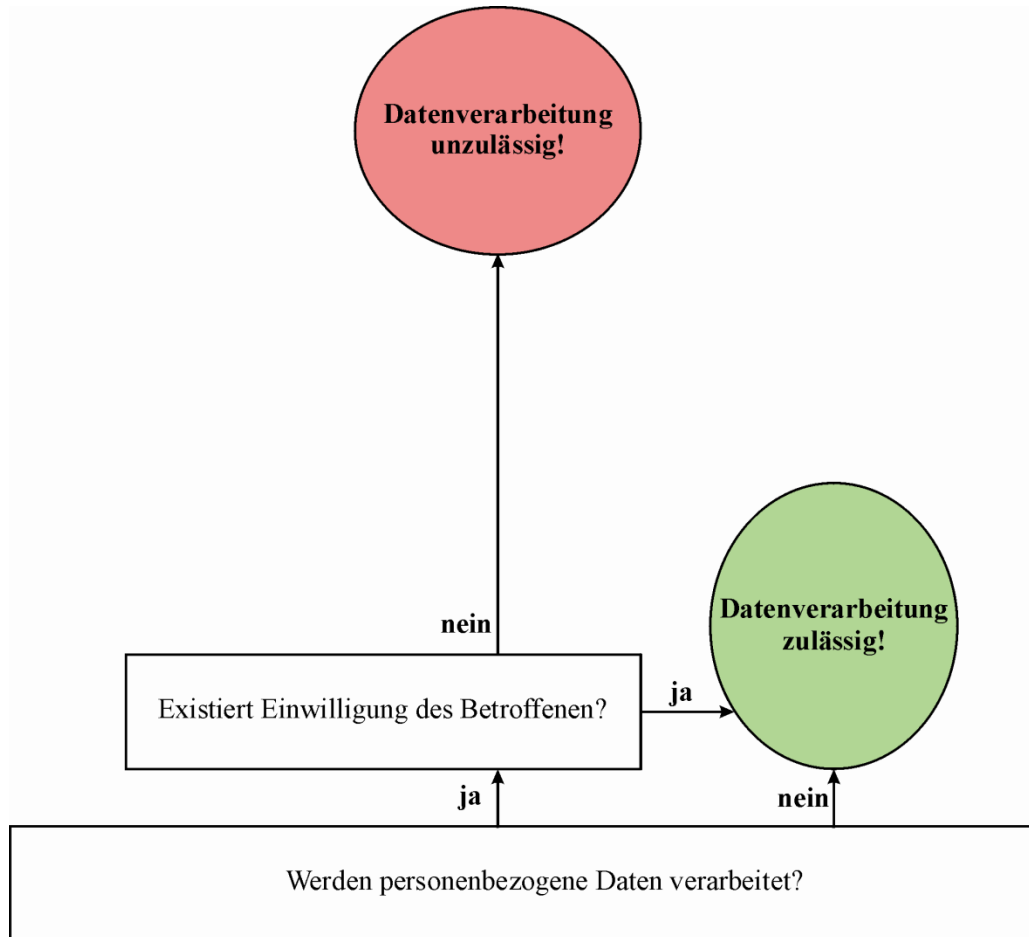


## Grundsatz:

Die Verarbeitung personenbezogener Daten ist grundsätzlich **verboten!**

Eine Gestattung ist jedoch unter Umständen möglich.

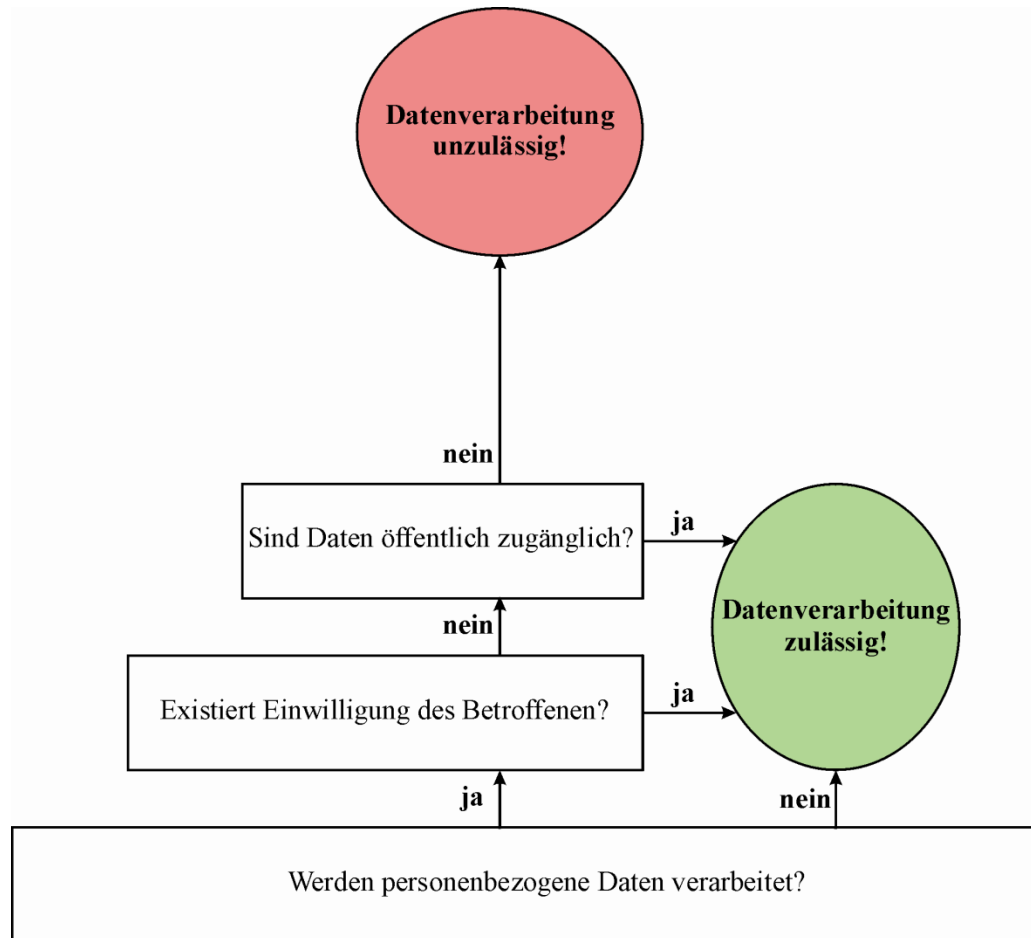
# Verbot mit Erlaubnisvorbehalt (2)



## Anforderungen an die Einwilligung:

- der Betroffene muss frei entscheiden können
- dem Betroffenen muss vorher der Zweck der geplanten Verarbeitung mitgeteilt werden
- der Betroffene soll über seine Rechte sowie die Folgen einer Ablehnung aufgeklärt werden
- die Einwilligung soll schriftlich erfolgen
- die Einwilligung ist jederzeit widerrufbar

# Verbot mit Erlaubnisvorbehalt (3)



## Öffentliche Quellen:

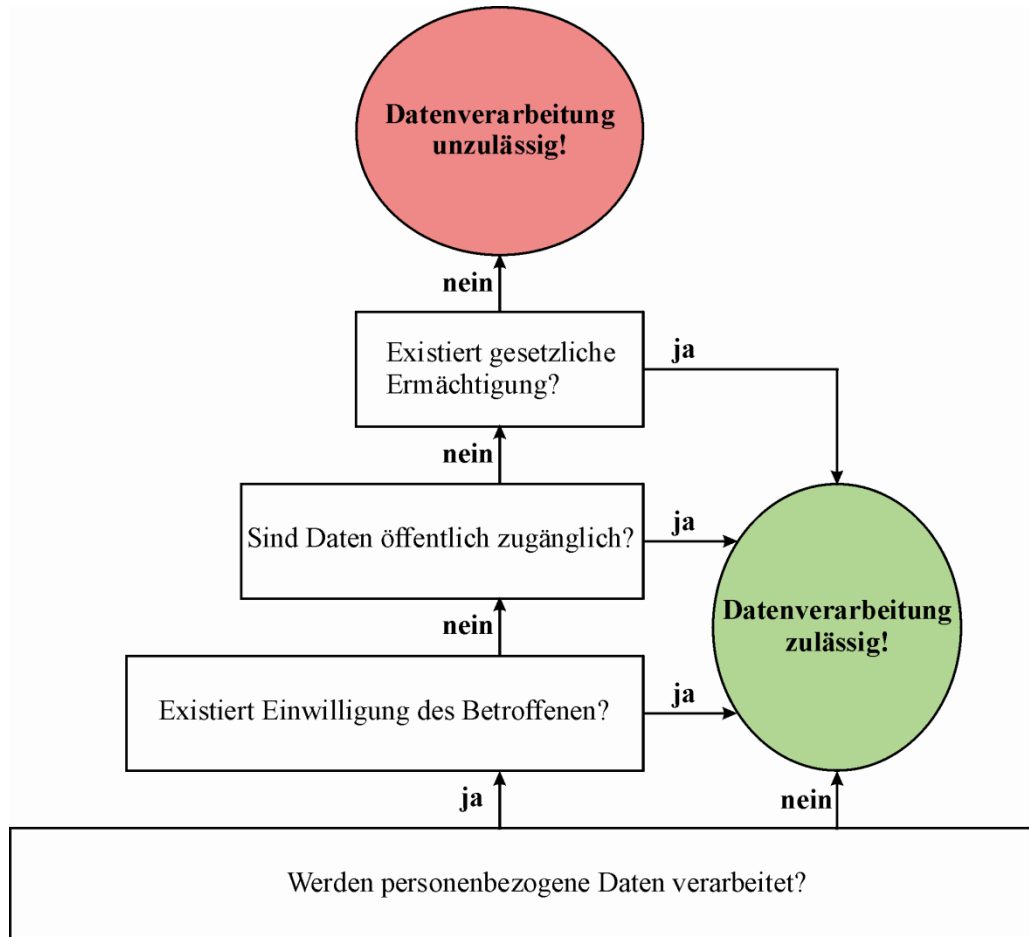
- Adress- und Telefonbücher
- öffentliche Register
- Veröffentlichungen
- Internet (sofern nicht passwortgeschützt)

## Hinweis:

- bei besonderen Arten personenbezogener Daten (z.B. Religionszugehörigkeit, Gesundheitsdaten) sind Daten nur öffentlich, wenn sie durch den Betroffenen selbst öffentlich gemacht wurden
- Unzulässig veröffentlichte Daten bleiben unzulässig
- Für Werbezwecke sind öffentliche Quellen auf Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse beschränkt



# Verbot mit Erlaubnisvorbehalt (4)



## Gesetzliche Erlaubnis:

- entweder im Datenschutzgesetz selbst
- oder in einer anderen Rechtsvorschrift (Gesetz, Verordnung, Satzung eines autonomen öffentlich-rechtlichen Verbandes mit gesetzlicher Ermächtigung), die verfassungsgemäß (normenklar und verhältnismäßig) ist

→ stellt **Regelfall** dar!  
(wg. Verweis auf rechtsgeschäftliches bzw. rechtsgeschäftsähnliches Schuldverhältnisses in § 28 BDSG)

# Verbot mit Erlaubnisvorbehalt (5)

Nach Art. 5 Abs. 1 lit. a der EU-DS-GVO müssen personenbez. Daten **auf rechtmäßige Weise und nach Treu und Glauben** verarbeitet werden

→ rechtmäßige Weise: im Einklang mit Art. 6 Abs. 1 der EU-DS-GVO:

- a) **Einwilligung** des Betroffenen für einen o. mehrere bestimmte Zwecke
- b) Erfüllung eines **Vertrags mit dem Betroffenen** bzw. zur Durchführung vorvertraglicher Maßnahmen auf Anfrage des Betroffenen
- c) Erfüllung einer **rechtlichen Verpflichtung** der verantwortlichen Stelle
- d) **Schutz lebenswichtiger Interessen** des Betroffenen oder einer anderen natürlichen Person
- e) Wahrnehmung einer **öffentlichen Aufgabe**, die der verantwortlichen Stelle übertragen wurde
- f) **Wahrung berechtigter Interessen** der verantwortlichen Stelle oder eines Dritten, sofern nicht die Interessen oder Grundrechte & Grundfreiheiten des Betroffenen zum Schutz personenbezogener Daten überwiegen (→ Abwägung nötig! Nicht auswählbar für Behörden)

→ Treu und Glauben: Vertrauensschutz (erfüllte gegenseitige Erwartung)

# Verbot mit Erlaubnisvorbehalt (6)

Nach Art. 9 Abs. 1 der EU-DS-GVO ist die **Verarbeitung besonderer Kategorien personenbezogener Daten verboten**, soweit nicht die Ausnahmen aus Art. 9 Abs. 2 der EU-DS-GVO greifen

Zu den besonderen Kategorien personenbezogener Daten zählen:

- Daten zur rassischen und ethnischen Herkunft
- Daten über politische Meinungen
- Daten über religiöse oder weltanschauliche Überzeugungen
- Daten über die Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder zur sexuellen Orientierung

# Verbot mit Erlaubnisvorbehalt (7)

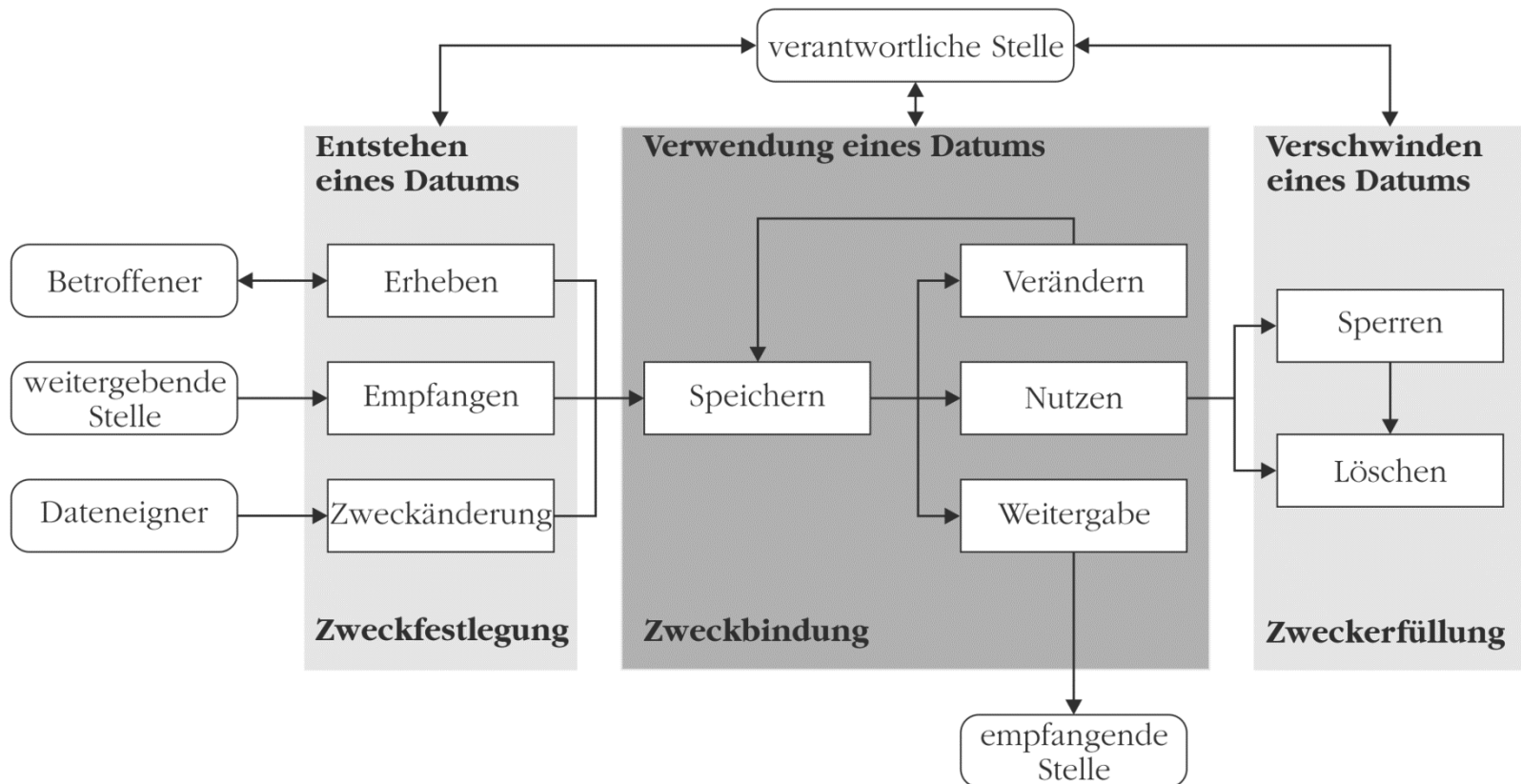
Zulässige **Ausnahmen** für Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 2 der EU-DS-GVO:

- a) Ausdrückliche Einwilligung des Betroffenen, soweit Einwilligung gesetzlich nicht verboten ist
- b) Erforderliche Angabe nach Arbeitsrecht, Recht der sozialen Sicherheit bzw. Sozialschutz
- c) Zum Schutz lebenswichtiger Interessen des Betroffenen bzw. einer anderen natürlichen Person, wobei der Betroffene aus körperlichen oder rechtlichen Gründen außerstande für Einwilligung sein muss
- d) Auf Grundlage einer geeigneten Garantie bei Tendenzschutzbetrieb
- e) Vom Betroffenen selbst offensichtlich öffentlich gemachte Daten
- f) Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- g) Vorgeschriebener Rechtsakt (EU-weit oder in Mitgliedsstaat)
- h) Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheits- bzw. Sozialbereich
- i) Öffentliche Gesundheit
- j) Archivierung im öffentlichen Interesse, wissenschaftliche oder historische Forschung bzw. Statistik (unter Berücksichtigung von Art. 89 der EU-DS-GVO)

# Prinzip der Zweckbindung

- Nach Art. 5 Abs. 1 lit. b der EU-DS-GVO müssen personenbezog. Daten für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht mehr zu vereinbarenden Weise weiterverarbeitet werden!
- Erfordernis zur **Zweckfestlegung** (Haupt- und Nebenzwecke) bei der Erhebung
- Zweck abhängig von geplanter **Verwendung**
- **Verfahren** (= *festgelegte Art & Weise, wie Tätigkeit / Prozess im Daten-Life-Cycle auszuführen ist*)  
im Datenschutzrecht kontextsensitiv/zweckabhängig  
→ zweckbezogen verknüpfte Verarbeitungsschritte
- Verarbeitungsschritte unterliegen **Zweckbindung**
- **Zweckänderung** nur bei berechtigtem Interesse unter Abwägung (→ abhängig vom Schutzgrad; muss mit ursprünglichen Zweck aber vereinbar sein!)
- teilweise existiert **besondere Zweckbindung**

# Verfahren (Daten Life Cycle)



# Prinzip der Transparenz

- Nach Art. 5 Abs. 1 lit. a der EU-DS-GVO müssen personenbezogene Daten in einer für die betroffene Person nachvollziehbare Weise verarbeitet werden!
- Betroffener muss folglich ihn betreffende Verfahren kennen
- Anlegen von **Verfahrensverzeichnissen** („Verzeichnis von Verarbeitungstätigkeiten“ nach Art. 30 Abs. 1 der EU-DS-GVO)
- **Informationspflicht** bei Direkterhebung beim Betroffenen (Art. 13 der EU-DS-GVO)
- **Benachrichtigungspflicht** bei fehlender Direkterhebung, inkl. Angabe, aus welcher Quelle Daten stammen (Art. 14 der EU-DS-GVO)
- **Auskunftsrecht** des Betroffenen (Art. 15 der EU-DS-GVO)
- **Einwilligung muss** von verantwortlicher Stelle **nachgewiesen werden** (Art. 7 Abs. 1 der EU-DS-GVO)
- Es existieren **besondere Informationspflichten** (z.B. bei Verletzung des Schutzes personenbezog. Daten sowie Logik & Tragweite Profiling)

# Zum Verzeichnisseverzeichnis (1)

- **jedes** einzelne Verfahren zur Verarbeitung personenbezogener Daten aufzuführen
- inhaltliche Anforderung aus § 4e BDSG (Meldepflicht gegenüber Aufsichtsbehörden, sofern kein Datenschutzbeauftragter bestellt wurde)
- Einsichtsrecht für **Jedermann**
- Unterteilung in öffentlichen Teil und nicht öffentlichen Teil
- der nicht öffentliche Teil (zu den Schutzvorkehrungen) unterscheidet sich bei nicht-öffentlichen Stellen (BDSG) von öffentlichen Stellen (jeweiliges LDSG bzw. BDSG)
- eine fundierte Datenschutzkontrolle erfordert detailliertere Angaben, als das Gesetz vorschreibt (Grund für Beschränkung: Betriebsgeheimnisse und Technikoffenheit!)



# Zum Verzeichnisseverzeichnis (2)

- BDSG benennt ausdrücklich einige Verfahren (Zwecke) und zeigt damit auf, welcher **Detaillierungsgrad** gefordert ist:
  - **Videoüberwachung** (§ 6b BDSG für öffentlich zugängliche Räume; für öffentlich nicht-zugängliche Räume gilt Auffangregel aus § 28 I Nr. 2 BDSG)
  - **Automatisierte Verarbeitung auf einem mobilen personenbezogenen Speicher- und Verarbeitungsmedium** (§ 6c BDSG)
  - **Automatisiertes Abrufverfahren** (§ 10 BDSG)
  - **Adresshandel** (§ 28 III BDSG)
  - **Werbung** (§ 28 III BDSG)
  - **Scoring** (§ 28b BDSG)
  - **Geschäftsmäßige Datenerhebung und –speicherung zum Zweck der Übermittlung** (§ 29 BDSG)
  - **Zwecke des Beschäftigungsverhältnisses** (§ 32 BDSG) [Plural!]
  - **Wissenschaftliche Forschung** (§ 40 BDSG)

# Zum Verzeichnisseverzeichnis (3)

Nach Art. 30 Abs. 1 der EU-DS-GVO ist Bestandteil des **Verzeichnisses von Verarbeitungstätigkeiten**:

- a) Angaben zur verantwortlichen Stelle und der zugehörigen Kontaktdaten (inkl. Datenschutzbeauftragter)
- b) Zwecke der Verarbeitung
- c) Kategorien der Betroffenen und personenbezogener Daten
- d) Kategorien von Empfänger
- e) Angaben zur Übermittlung in Drittländer oder internationalen Organisationen
- f) Lösungsfristen je Datenkategorie
- g) Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (nach Art. 32 Abs. 1 der EU-DS-GVO)

Davon unterliegen a) bis f) den Informationspflichten gegenüber dem Betroffenen; f) im Sinne von geplanter Speicherdauer.

# Direkte Überwachung / Sammlung

	Beschäftigte	Kunden
<b>Fähigkeiten</b>	Personalentwicklung Qualitätsmanagement	Kauf technischer Produkte
<b>Leistung</b>	Betriebsdatenerfassung	Trainingsapps
<b>Verhalten</b>	Zutrittskontrolle Videoüberwachung Arbeitszeitüberwachung Internet-Nutzungs-Kontrolle Einzelverbindungs-nachweis	Rabattsysteme Videoüberwachung Videoconferencing Customer Relationship Management (CRM) Webtracking

- Eine direkte Überwachung kann der Betroffene i.d.R. feststellen
- Hier kann der Betroffene oft aktiv entscheiden, ob er etwas und was genau er über sich preis gibt (bzw. geben muss)  
→ Oftmals aber keine echte Freiwilligkeit...

# Indirekte Überwachung / Sammlung

	Beschäftigte	Kunden
<b>Fähigkeiten</b>	Mitarbeitergespräche	Bonitätsprüfung
<b>Leistung</b>	Projektmanagement Ressourcenmanagement	Kundenhistorie
<b>Verhalten</b>	Ticketsysteme Computer Supported Cooperative Work (CSCW) Soziale Netzwerke Unified Communications Anti-Terrordaten-Abgleich	Bewegungsprofile Geotagging Kaufprognosen Scoring eingebundene Werbung TK-Überwachung Nachrichtendienste

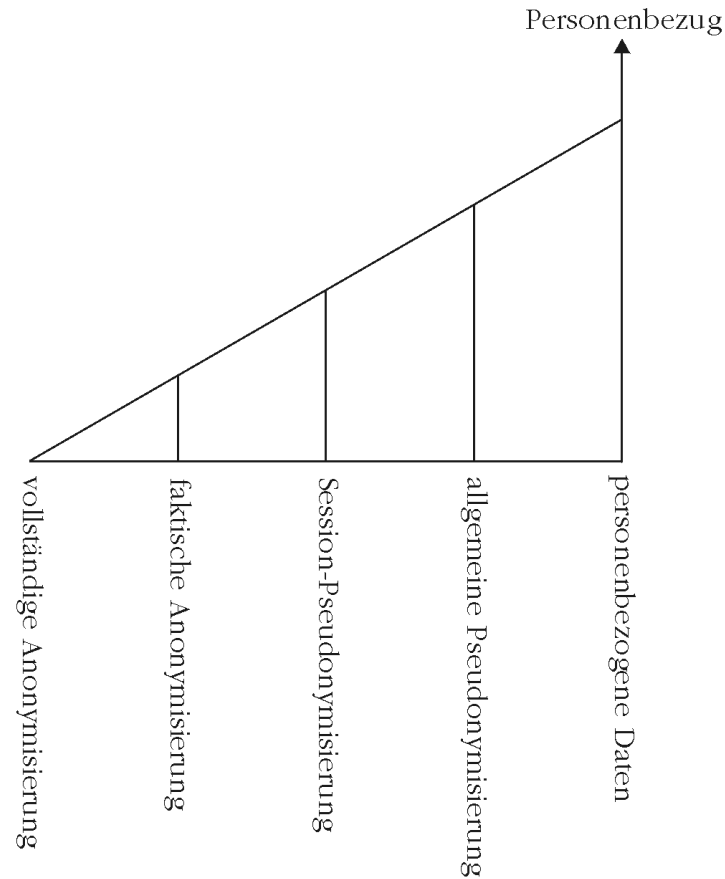
Big Data

- Indirekte Überwachungen dagegen nur eingeschränkt feststellbar
- Oft basierend auf Zweckänderung/-erweiterung
- Hier ist ein gesetzlicher Ausgleich nötig! (fehlt bisher leider...)

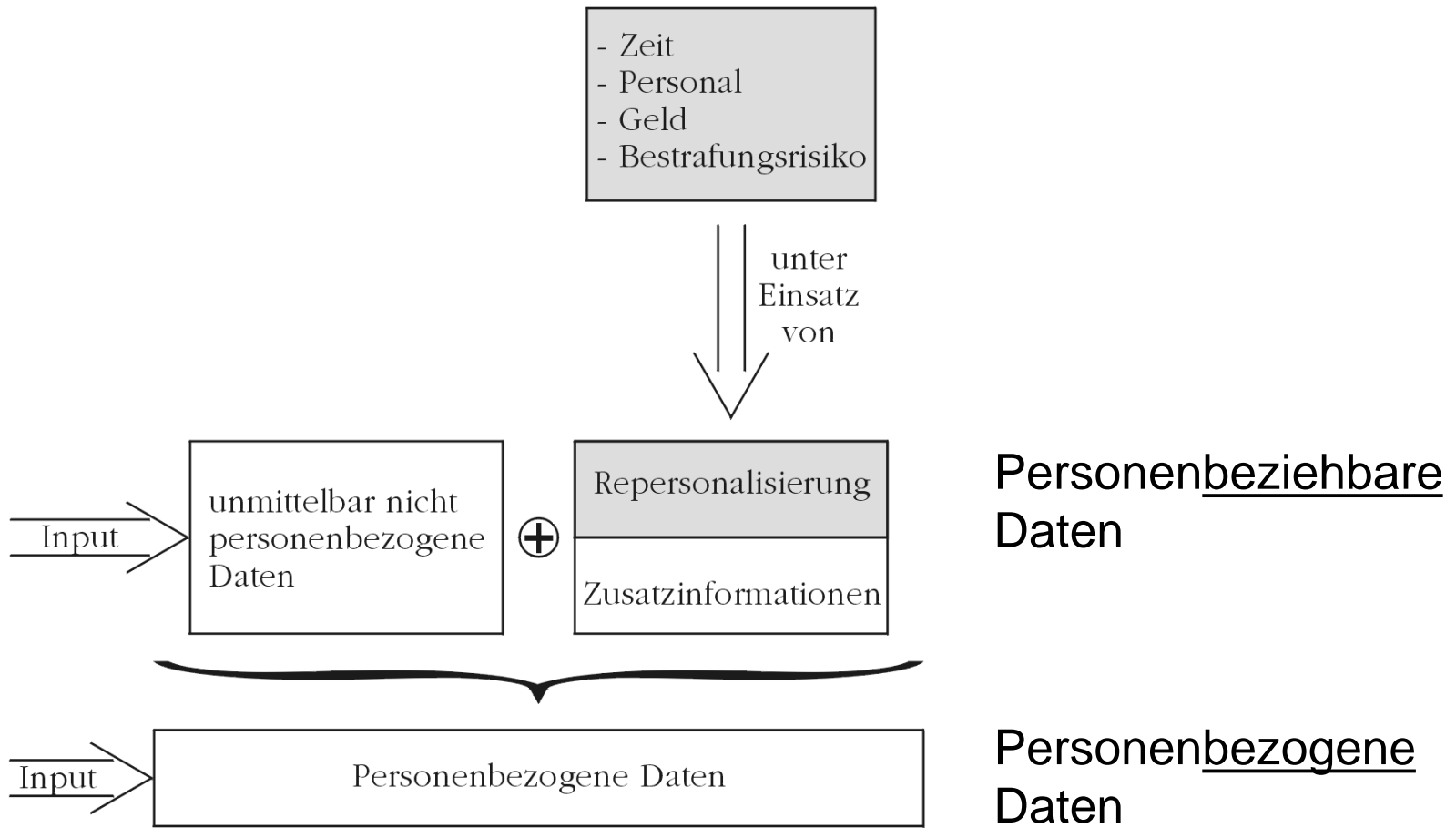
# Prinzip der Datenminimierung (1)

- Nach Art. 5 Abs. 1 lit. c müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein
- Anforderung zur **Gestaltung** der eingesetzten IT-Systeme (maßgeblich für privacy by design)
- Verbot **unnötiger Vorratsdatenhaltung**
- **Vermeidung** des Personenbezugs, sofern dieser nicht unbedingt (zur Erfüllung des Verwendungszwecks unmittelbar) erforderlich ist
- Verwendung **datenschutzfreundlicher Techniken**
- Ermöglichung **anonymer** und **unbeobachteter** Nutzung von Telemedien
- Betrifft alle Phasen der automatisierten Verarbeitung

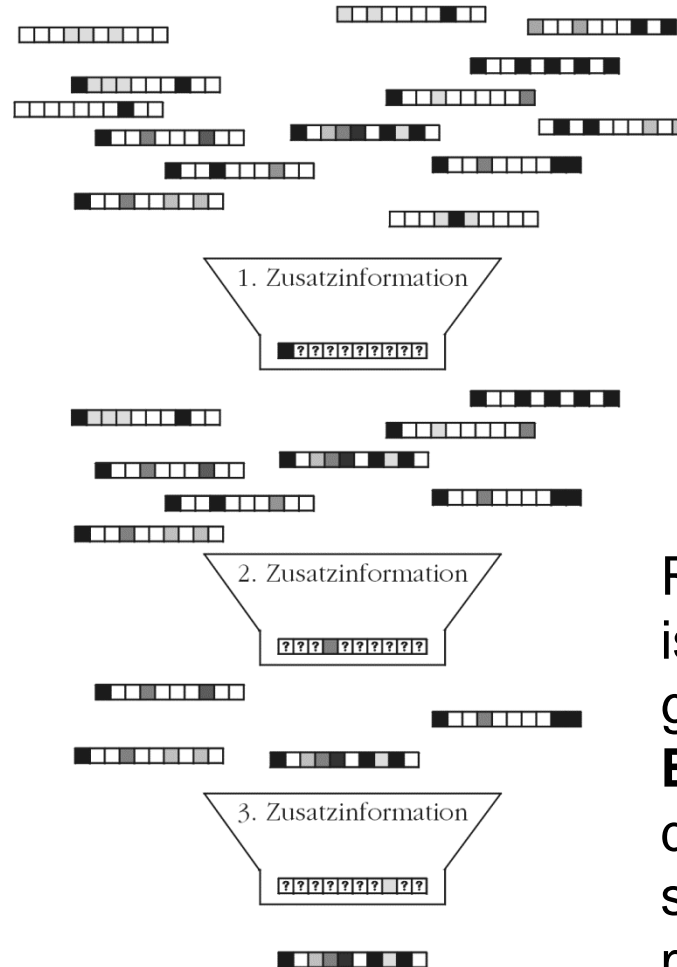
# Prinzip der Datenminimierung (2)



# Repersonalisierung (1)



# Repersonalisierung (2)



Repersonalisierung ist zugleich die größte Gefahr bei **Big Data** aufgrund der zur Verfügung stehenden Datenmenge!



# Prinzip der begrenzten Speicherung

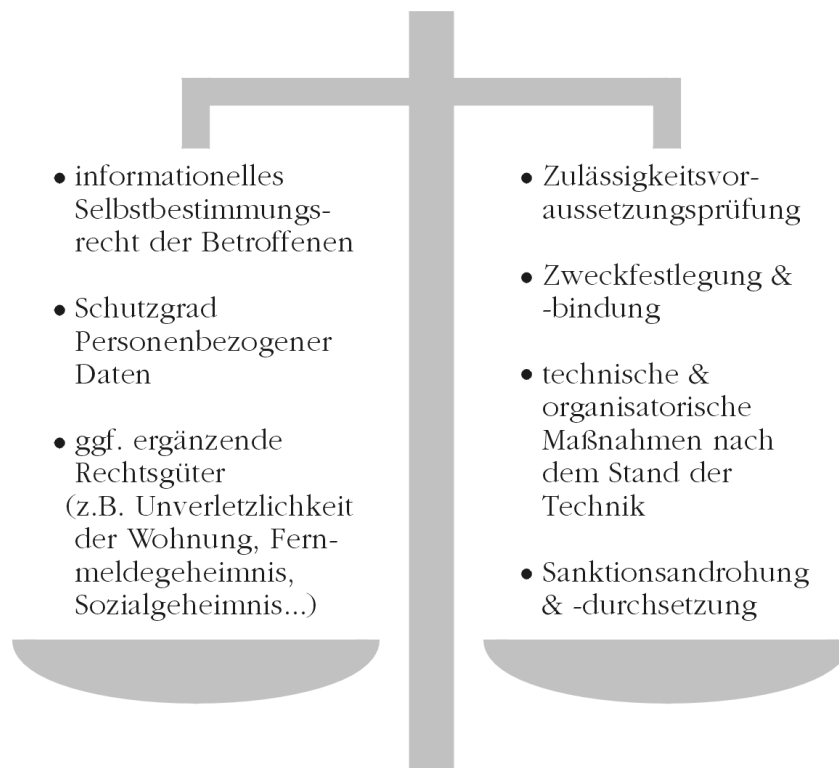
- Nach Art. 5 Abs. 1 lit. e der EU-DS-GVO müssen personenbezogene Daten in einer Form gespeichert werden, die die **Identifikation der betroffenen Personen nur so lange** ermöglicht, **wie** es für die Zwecke, für die sie verarbeitet werden, **erforderlich** ist
- An vielen Stellen der EU-DS-GVO wird daher ausdrücklich eine Pseudonymisierung der Daten eingefordert:
  - Erleichterung bei Zweckänderung (Art. 6 Abs. 4 lit. e)
  - Einschränkung bei Auskunftsrechten (Art. 12 Abs. 2)
  - Umsetzung von Privacy by Design bzw. by Default (Art. 25)
  - Empfohlene Maßnahme zur Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. a)

# Verhältnismäßigkeitsprinzip (1)

- Abstufung zwischen **erforderlich** (um Aufgaben rechtmäßig, vollständig & in angemessener Zeit erfüllen zu können) und **zwingend** (unerlässlich für Aufgabenerfüllung)
- maßgeblich ist der **Einzelfall**
- **geringerer Eingriff** ins informationelle Selbstbestimmungsrecht vorrangig (z.B. mittels Anonymisierung)
- Je **weniger** eine automatisierte Verarbeitung unter **Einfluss** des Betroffenen stattfindet, **desto mehr Gewicht haben** seine **Schutzrechte** (§ 28 II Nr. 2 BDSG schärfere Abwägung als § 28 I Nr. 2 BDSG)
- Automatisierte Verarbeitung nach „**Treu und Glauben**“
- Beachtung von **Schutzgraden** & technischem / organisatorischem Ausgleich (**Zumutbarkeit**)
- öffentliche Stelle restriktiver als nicht-öffentliche (da Abwehrrecht statt mittelbarer Wirkung)

# Verhältnismäßigkeitsprinzip (2)

- **Eingriffe** in Grundrechte müssen **verhältnismäßig** sein  
(= **geeignet, erforderlich & angemessen**)
- **Sonst:**  
Schmerzensgeld bei unverhältnismäßiger Videoüberwachung von Beschäftigten:
  - Hess. LAG 2010: 7.000 €
  - LAG Berlin 2012: 14.000 €
  - AG Frankfurt 2013: 3.500 €



# Weitere Regelungen zum Datenschutzrecht

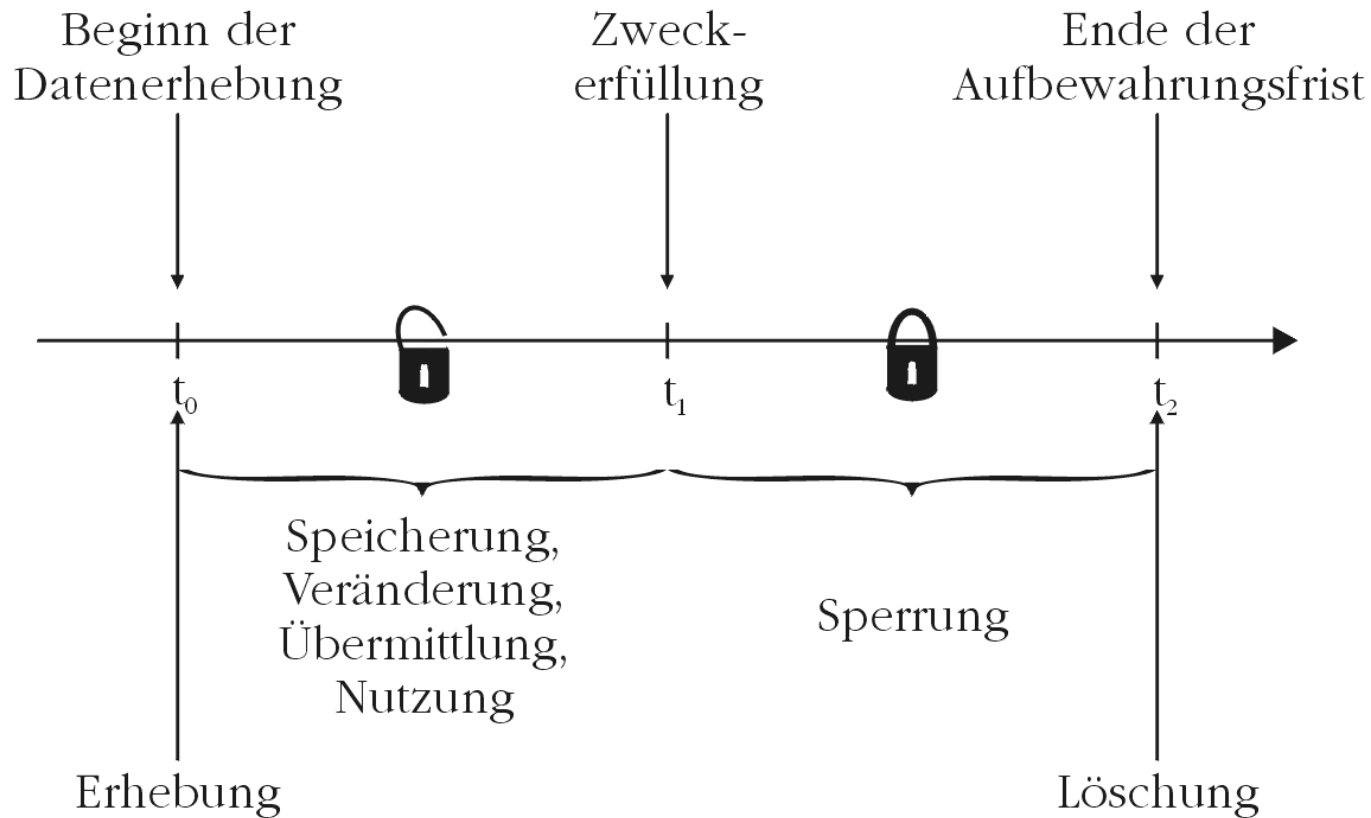
- Gewährleistung der **Betroffenenrechte**
- **Abgrenzungen:** [→ Übungen!]
  - Übermitteln vs Nutzen
  - Auftragsdatenverarbeitung vs Funktionsübertragung
- Verpflichtung der DV-Durchführenden auf das **Daten-  
geheimnis** [ohne Folie]
- **Datenschutzkontrolle:**
  - Selbstkontrolle durch Betroffene
  - Eigenkontrolle durch Datenschutzbeauftragte
  - Fremdkontrolle durch Aufsichtsbehörde

# Betroffenenrechte

- Recht auf **Auskunft** (Art. 15)
- Recht auf **Berichtigung** unrichtiger personenbezogener Daten (Art. 16)
- Recht auf **Löschung** unzulässiger personenbezogener Daten, nicht mehr zur Zweckerfüllung notwendiger Daten, Daten aus Einwilligungserklärungen nach deren Widerruf, Daten nach eingelegtem Widerspruch gegen Profiling (soweit kein überwiegendes berechtigtes Interesse dagegen steht) bzw. rechtlich vorgeschriebener Löschung (Art. 17 Abs. 1), soweit nicht zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt (Art. 17 Abs. 3)
- Recht auf **Sperrung** nicht mehr benötigter personenbezogener Daten
- Recht auf **Anrufung** des Datenschutzbeauftragten (Art. 38 Abs. 4)
- Recht auf **Beschwerde** bei Aufsichtsbehörde (Art. 77)
- Recht auf **Schadenersatz** (Art. 82)
- Neu (Art. 21): **Widerspruchsrecht** gegen Profiling und Direktwerbung
- Neu (Art. 20): Recht auf **Datenübertragbarkeit**

Niemand darf wegen der Geltendmachung seiner Rechte benachteiligt werden!

# Löschung & Sperrung von Daten

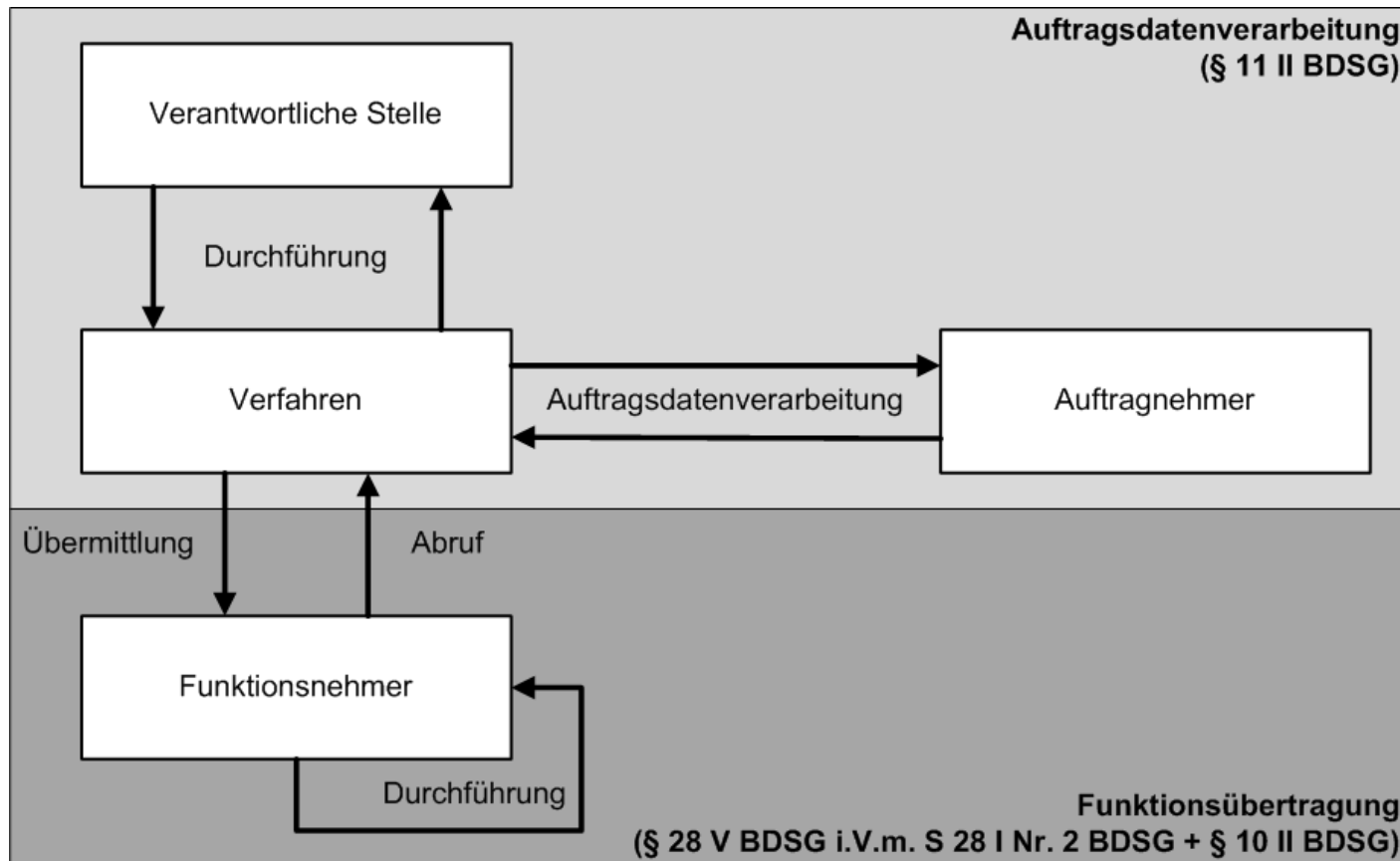


# Auftragsdatenverarbeitung vs Funktionsübertragung (1. Ergänzung)

## Zuordnungsproblematik beim Cloud Computing

- Beim Cloud Computing wird
    - Infrastruktur (Hardware, physischer Speicher, ...)
    - Plattformen (Datenbanksysteme, Run-Time Environment, ...)
    - Software (Applikationen, CRM-Systeme, ...)skalierbar & verteilt i.d.R. gegen Entgelt zur Verfügung gestellt
  - § 11 BDSG erfordert präzise Kenntnisse des Auftraggebers über die Auftrags erledigung durch Auftragnehmer (Kontrollrecht)
  - Beim Cloud Computing sind dagegen die Details „wolkig“, obwohl ansonsten von einer klassischen Auftragsdatenverarbeitung auszugehen wäre
- SLAs & Audits; aber: eingeschränktes Weisungsrecht → ???

# Auftragsdatenverarbeitung vs Funktionsübertragung (2. Ergänzung)





# Der Datenschutzbeauftragte (1)

## Aufgaben von Datenschutzbeauftragten (nach dem BDSG):

- **Hinwirken** auf die Einhaltung datenschutzrechtlicher Vorschriften
- datenschutzrechtliche und -technische **Überwachung** der automatisierten Datenverarbeitung, mit der personenbezogene Daten verarbeitet werden
- datenschutzrechtliche **Schulung** der Personen, die personenbezogene Daten verarbeiten & Verpflichtung dieser auf das Datengeheimnis (IT, Personalabteilung, Poststelle, Empfang, Betriebsdatenerfassung, ggf. Vertrieb)
- **Mitwirkung** bei Abschluss von Verträgen, Betriebsvereinbarungen, Policies und Dienstanweisungen
- **Ansprechpartner** für Betroffene (→ Prüfung von Beschwerden)
- Durchführung der **Vorabkontrolle** bei besonders riskanten automatisierten Verarbeitungen

# Der Datenschutzbeauftragte (2)

**Aufgaben von Datenschutzbeauftragten** (nach Art. 39 der EU-DS-GVO):

- **Unterrichtung** und Beratung der verantwortlichen Stelle (bzw. des Auftragnehmers) und der die Verarbeitung durchführenden Beschäftigten **hinsichtlich ihrer Pflichten zum Datenschutz**
- **Überwachung der Einhaltung** der Datenschutzvorschriften
- **Beratung (auf Anfrage!)** im Zusammenhang mit der durchzuführenden **Datenschutz-Folgenabschätzung**
- **Überwachung der Durchführung der Datenschutz-Folgenabschätzung**
- **Zusammenarbeit mit der Aufsichtsbehörde**

Dabei trägt der Datenschutzbeauftragte dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung (unter Berücksichtigung von Art, Umfang, Umstände und Zwecke der Verarbeitung).

# Der Datenschutzbeauftragte (3)

## Anforderungen an Datenschutzbeauftragte:

- **Fachkunde:** Datenschutzrecht, Datenverarbeitung, betriebliche Organisation, Didaktik, Psychologie [Urteil des LG Ulm, 1990]
- **Zuverlässigkeit:** Verschwiegenheit, ohne Interessenkonflikte, charakterliche Eignung
- nur natürliche Person kann bestellt werden

## Absicherung des Datenschutzbeauftragten:

- unmittelbar der Geschäftsführung unterstellt
- Weisungsfreiheit
- Benachteiligungsverbot → Kündigungsschutz
- Unterstützung durch Unternehmen

# Der Datenschutzbeauftragte (4)

## **Typische Tätigkeiten eines Datenschutzbeauftragten:**

- Recherchen zur aktuellen Rechtslage (Auswertung aktueller Urteile)
- Lesen & Auswerten zahlreicher & umfangreicher Fachartikel & Fachliteratur
- Vorbereitung von & Teilnahme an & Protokollierung der Meetings (Geschäftsführung, IT-Leitung, Fachverantwortliche)
- Erstellung von Stellungnahmen & Verfahrensverzeichnissen
- Durchführung & Dokumentation von Vor-Ort-Kontrollen & Vertragskontrollen (u.a. zur Abgrenzung einer Auftrags-DV)
- Durchführung von Vorabkontrollen bei kritischen DV
- Erstellung & Begutachtung von Sicherheitskonzepten
- Planung & Durchführung von Mitarbeiterschulungen
- Gespräche mit Aufsichtsbehörden

# Der Datenschutzbeauftragte (5)

## **Unerfreuliche Erfahrungen eines Datenschutzbeauftragten:**

- komplexe Materie erfordert permanente Erneuerung der Informationsbasis
- verspätete Information (z.B. durch nachzuholende Vorabkontrolle) hat Mehrarbeit & Mehrkosten zur Folge
- Eigenschaft als Miesmacher gegenüber „schöner neuer Welt“
- Abwägungserfordernis führt teilw. zu fehlender Trennschärfe
- Feststellung von Fehlverhalten wichtiger Mitarbeiter & von strukturellen Defiziten
- festgestellte Datenschutzverstöße teilweise Kündigungsgrund von Mitarbeitern
- Durchsicht von Festplatten mit (Kinder-) Pornographie
- Anrufung mit Ziel der Verhinderung arbeitsrechtlicher Aufklärung

# Checks & Balances bei der Datenschutzkontrolle

